ANALYSIS OF HOW SERBIAN INSTITUTIONS FUNCTION IN THE FIGHT AGAINST ORGANISED CYBERCRIME

WESTERN BALKANS ORGANIZED CRIME RADAR

BCSP

ANALYSIS OF HOW SERBIAN INSTITUTIONS FUNCTION IN THE FIGHT AGAINST ORGANISED CYBERCRIME

March 2021.

Publisher
Belgrade Centre for Security Policy (BCSP)
Address: Đure Jakšića 6/5, Belgrade, Serbia
Website: www.bezbednost.org
Email: office@bezbednost.org

Author
Marija Pavlović

Editor
Tatjana Hadžić Jovović

Design and Layout
Srđan Ilić

Translation
Ivan Kovanović

Kingdom of the Netherlands

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND

Norwegian Embassy
Belgrade

The views expressed in this publication do not represent those of the Royal Norwegian Embassy in Belgrade, the Balkan Trust for Democracy, the German Marshall Fund of the United States of America or of their partners.

Introduction

This study seeks to contribute to a better understanding of the fight against cybercrime in Serbia, as well as understanding of the links between organized and cybercrime. The study analyses data obtained from strategic documents of the Republic of Serbia, as well as legislation that pertains to cybercrime or is otherwise closely related to this field. In addition to this, the study also involved interviews with experts in this field. It ought to be noted that most institutions failed to respond when invited to participate in these interviews, including the main actor in the fight against cybercrime, the Ministry of Interior (*Ministarstvo unutrašnjih poslova*, MUP). The main finding of this study is that, from 2005 to the present, Serbia did much to regulate the legislative framework in this area, the most significant developments being the formation of a special police unit and a unit within the prosecutor's office for combating cybercrime. Although experts agree that this area is now well regulated in terms of legislation, in practice there remain numerous issues that will be covered in more detail in this paper.

Cybercrime is a form of criminal activity that is continually expanding, and that is one of the most dangerous security challenges in the world today. Although it brings with it many benefits, the rapid development of information technology and its increasingly significant presence in all spheres of contemporary society also contributes to the spread of cybercrime. There has been a noticeable increase in cyber-related crimes in Serbia. The Ministry of Interior's Information Booklet states that 622 crimes in this area were committed in 2018, while in 2019 this figure was 946.[1] The key reasons for the rise in this kind of criminal activity lie in the increased access to the Internet and increasing numbers of people using social media, mobile devices, and other applications that enable various forms of communication. Detecting and investigating these kinds of crimes can be difficult because the crimes can be committed in different geographical locations in real time. In other words, the perpetrator, the victim, and the means of committing the crime can be in different parts of the world at the same time. As with other forms of criminal activity, cybercrime can also involve a level of organization. This is best illustrated through the example of one of the largest criminal organizations on the Internet, *Infraud*.[2] This organization was discovered and dismantled in 2018, as part of *Shadow Web*, an international police operation. The Serbian police participated in *Shadow Web*, which resulted in 36 suspects being charged – including one Serbian citizen.[3]

This paper consists of three sections. The first of these analyses the legislative and institutional framework in Serbia, as well as the frameworks governing the forms of international, regional, and national cooperation in which Serbia participates. The second part of the paper examines links between cybercrime and organized crime. Finally, the paper provides recommendations for tackling the issues that have emerged in practice.

Analysing the Legislative and Institutional Framework

This section analyses the most important laws that govern the fight against cybercrime. In order to improve the legislative framework, Serbia opted for partial, targeted amendment of certain laws. In addition to these partial legislative amendments, Serbia has also passed a new law, which forms new governmental bodies for dealing with this type of criminal activity.[4] Namely, the Law on Organisation and Competences of Government Authorities Responsible for Combating High Technology Crime.[5] This law specifies which institutions are tasked with combating cybercrime, how their activities are regulated and what their powers are. Partial, targeted amendments were made to, among others, the Criminal Code[6] and the Criminal Procedure Code[7]. The Criminal Code defines which criminal acts can be characterized as cybercrime, as well as the penalties envisaged for the commission of these offenses. The Criminal Procedure Code prescribes a slew of special evidentiary actions that can be deployed in investigating these types of crimes. Both of these documents provide definitions of terms significant to the field of cybercrime.

The Serbian state has placed great emphasis on the fight against cybercrime, as can be seen from the strategic documents it has drafted. One essential document in this area is the Strategy for the Fight Against Cybercrime for 2019-2023, adopted in September 2018 together with an Action Plan for implementing this strategy for the period 2019-2020.[8] This strategy defines the rights and obligations of all actors tasked with combating cybercrime in Serbia. It also lists all of the institutions that are charged with participating in effective suppression of cybercrime, in line with the strategic and operational elements of EU accession. The strategy aims to establish an effective and sustainable system that unifies the operations of all institutions tasked with combating cybercrime.[9]

The Law on Organisation and Competences of Government Authorities Responsible for Combating High Technology Crime establishes the Special Prosecution Office for High Tech Crime. This office is part of the Higher Public Prosecutor's Office in Belgrade, but it has a national-level jurisdiction. According to the cybercrime strategy, in addition to the special prosecutor's office, the Higher Court in Belgrade is also empowered to handle cybercrime cases across the territory of Serbia, while the Court of Appeals in Belgrade will adjudicate on appeals. As of 2009, however, the Higher Court of Belgrade no longer has a specialized department for these crimes.[10] With the abolishment of this specialized department, all judges of the Higher Court in Belgrade can adjudicate on cybercrime cases, and all panels of the Court of Appeals in Belgrade can hear case appeals. As a result of this decision, problems have emerged in practice – such as that these cases are being tried by judges who have hitherto only tried more general criminal cases. The insufficient training of judges for hearing trials of such cases, who are not well-acquainted with terminology that pertains only and exclusively to cybercrime, can lead to difficulties with such trials.[11]

The Ministry of Interior has, for its part, established a special Department for Cybercrime within its Service for Combating Organised Crim (*Služba za borbu protiv organizovanog kriminala* – SBPOK). The Department is the most important link in the chain of combating cybercrime since it takes on all cases that contained elements of cybercrime.

In 2019, it was divided into four subsections: the Section for Intellectual Property Crime, the Section for Electronic Crime, the Section for Illicit and Harmful Content on the Internet, and the Section for E-Commerce, E-Banking, and Payment Card Crime on the Internet.[12] The Department acts on requests of the Special Prosecution Office for High Tech Crime, which manages pre-investigative procedures in these cases, but it also responds to requests by other prosecutor's offices as needed.[13] When it comes to organized forms of cybercrime, the Department acts on the orders of the SBPOK, and such crimes fall under the jurisdiction of the Prosecutor's Office for Organized Crime.

Why is this subdivision within the Department important? The very complexity of this kind of crime requires specially trained personnel, who are in turn able to work exclusively on these types of offenses and who will be organized in such a way that they will not be overworked and so that certain cases will not be neglected. Due to the specialized nature of these roles, the police and prosecution lack the requisite capacities and human resources. Even though the strategy and action plan for this area resulted in increases to personnel in this department over the past two years, the overall numbers remain inadequate.[14] Each section within the Department is intended to work exclusively on cases within its specialised purview but, in practice, this has not proven to be the case. According to data from the Statistical Office of Serbia, certain types of general criminal offenses are more prevalent than offenses that fall exclusively within the jurisdiction of the body tasked with combating cybercrime.[15]

> “ *The police and prosecution are mostly engaged with the criminal offense of endangerment of safety via social media, which is wholly inappropriate and which is reflected in the statistical data when it comes to offenses against computer systems. You get circumstances in which the prosecution and police engage in investigation of certain acts that, according to the letter of the law, they should not investigate. By doing this, they use up their precious time and resources working on something party political. And, in that sense, the police's lack of operational autonomy comes to the fore. Meanwhile, the prosecution did not prove itself to be particularly resistant to pressure, especially public pressure, when it comes to social media goings on.*[16]

This kind of politicization of the police affects the activities and expediency of the Department, whose capacities are focused on the criminal offense of endangerment of safety via social media, rather than on the tasks for which they are trained, which is a waste of resources. According to the EUROPOL "Internet Organised Crime Threat Assessment 2020", the amount of online child sexual abuse material continues to increase.[17] This increase seriously impacts the capacities of police and prosecution services everywhere in the world, including Serbia. These are not, however, the only offenses on the rise. Crimes targeting data security are also on the increase. Due to insufficient human resources and a lack of operational autonomy for the police and prosecutor's offices, serious criminal offenses can go unchecked.

In addition to the bodies covered above, the cybercrime strategy also envisages the formation of special cybercrime departments as part of the Security Information Agency (*Bezbednosno-informativna agencija*, BIA) and the Military Security Agency (*Vojnobezbednosna agencija*, VBA).[18] The Security Information Agency is tasked with combating all types of cybercrime if it is deemed that this can destabilise national security, in accordance with the Law on the BIA.[19] In accordance with the Law on the VBA and VOA, the Military Security Agency acts to detect, prevent and investigate criminal offenses against data security.[20] It has powers to provide data security for the IT systems of the Armed Forces of Serbia and the Ministry of Defence.[21]

Cooperation through all channels of international police cooperation, via INTERPOL and EUROPOL, is ongoing. An international point of contact has been established within the Department for Cybercrime that is available 24 hours a day, seven days a week – enabling cybercrime cooperation as part of a Council of Europe framework. International cooperation is crucial since most of the service providers used to perpetrate offenses are located beyond Serbia's borders. At the national level, to further advance the fight against cybercrime, it is essential that better cooperation is established between the private, public, and civil sectors.

Cybercrime as a Form of Organized Crime

The term organized crime refers primarily to profit from a continuation of business practices by criminal means. Accordingly, organized crime groups are behaving in a manner reminiscent of modern corporations and are, in search of new opportunities to turn a profit, moving their business online. Organized criminal groups strive to better identify and take advantage of opportunities for new illegal activities and enterprises. In this context, the internet and continued growth of e-commerce present enormous new prospects for illegal financial gain.[22] These groups are not even forced to develop technical expertise and can instead employ any individuals from the hacker community who possess the knowhow to perform the relevant tasks.

Organized cybercrime has not been sufficiently explored as a topic in Serbia, nor indeed globally, hence many aspects of this kind of criminality remain opaque. One possible reason for this could be that perpetrators of cybercrime are mostly assumed to be loners who have the knowledge and skillset necessary to commit such crimes for personal gain. Today, however, there are various forums and online communities where hackers can come together to share their experiences and exchange knowhow, but also where they can find accomplices to commit certain crimes. With the advancement of technology and growing use of new technologies, new organized criminal groups are emerging and operating in cyberspace.

Two kinds of organized crime networks that operate in the virtual sphere have been identified.[23] The first is cybercrime as a new way of conducting organized crime. It refers to traditional organized crime networks using information technology to improve on their usual criminal activities. The best example of this in Serbia can be gleaned from statements by government officials that the criminal group headed by Veljko Belivuk (aka Velja Nevolja) used special encrypted mobile phones and the Sky application to communicate with one another. Evidence of several serious offenses was found on these phones.[24]

The second type of network is cybercrime as a new form of organized crime. These are organized criminal groups that operate exclusively on the Internet, whose members are highly tech-savvy. The members of such groups typically know one another only via the Internet and their virtual avatars.[25] They meet, communicate and plan their criminal activities exclusively online. These groups are usually loosely structured, they tend to be smaller, and it is more likely that their members are not located in one country but are scattered across the globe. Such groups are less hierarchical than traditional organized crime groups. The actors participating in such groups do not have to be geographically concentrated, formally organized, or united by a common system of values. An example is the *Infraud* organized criminal group, which operated exclusively on the Internet. This organization procured and peddled stolen data – including data from compromised payment cards, the personal data of individuals, and the financial data of both individuals and companies – and also engaged in the production and distribution of malware and the like.[26]

From the above it can be concluded that the relationship between cybercrime and organized crime can be understood in two ways: As a new form of organized crime that takes place exclusively on the Internet and as a new way of using modern technology in the service of more traditional forms of organized crime. This relationship is important because it dictates which police units and which prosecutor's office will be tasked with investigating these criminal offenses. This creates problems of jurisdiction and coordination between the Prosecutor's Office for Organised Crime and the Special Prosecution for High-Tech Crime, hence it is important how the relationship is defined.

Conclusion

The transfer of commerce to the online sphere and the mass use of computers and mobile devices will increase the likelihood of these technologies being abused for criminal purposes, which will lead to an increase in this kind of crime. Raising public awareness of the dangers that lurk in the virtual world plays an extraordinary role in the prevention of cybercrime. Among other things, this means improving people's knowledge about how to protect their personal data and how to conduct their business online. Digital literacy is also very significant in terms of prevention, since it is increasingly common that people do not know how the technology they use works.

In the virtual world, as in its real world counterpart, most criminal acts are perpetrated by individuals or small groups in a manner that can be best described as 'unorganized crime'. Even though evidence is mounting that organized criminal groups use the new opportunities offered by the Internet, organized crime and cybercrime are unlikely to ever become synonymous. Most organized crime will continue to unfold in the real world, and most cybercrime will continue to be perpetrated by individuals rather than criminal networks. Even so, the level of overlap between these two phenomena will likely increase in the coming years.[27] Consequently, for the fight against cybercrime to continue to advance, it is imperative that cooperation and coordination continue to take place, both internationally and at the national level.

Recommendations

The human resources of the Department for High-Tech Crime need to be increased, as does the office space available to the Special Prosecution for Combating High-Tech Crime .

Continued training is needed for the judges and lawyers who come into contact with this kind of material so as to avoid problems with proceedings that arise from insufficient understanding of the subject matter.

Greater cooperation between the private, public, and civil sectors is needed at the national level so as to further advance the fight against cybercrime. This cooperation must be continuous, as the technology in this area, as well as the accompanying security challenges, risks, and threats, are constantly evolving.

Greater operational autonomy for the Department for High-Tech Crime and the Special Prosecution for Combating High-Tech Crime is imperative.

Sources

[1] Ministry of Interior, *Informator o radu za avgust 2020. godine* (Information Booklet for August 2020), p. 129, available at: http://www.mup.gov.rs/wps/wcm/connect/31d27fcf-403e-4620-9380-0b9563645b40/IOR%2Bavgust%2Bcirilica2020..pdf?MOD=AJPERES&CVID=ng6-nli, accessed: 17/03/2021.

[2] CNN, *International cyber crime ring smashed after more than $530 million stolen*, 2018, available at: https://edition.cnn.com/2018/02/08/world/us-cyber-crime-ring-arrests-intl/index.html, accessed: 17/03/2021.

[3] Ministry of Interior, *Procena pretnje od teškog i organizovanog kriminala – SOCTA* (Serious and Organised Crime Threat Assessment – SOCTA), 2019, p. 113, available at: http://www.mup.gov.rs/wps/wcm/connect/fb61b551-a863-42b3-a208-53892082f851/SOCTA+2019+-+Procena+pretnje+od+teskog+i+organizovanog+kriminala.pdf?MOD=AJPERES&CVID=nl6aHQ2, accessed: 17/03/2021

[4] Komlen Nikolić, L. et. al. 2010. *Suzbijanje visokotehnološkog kriminala* (Supressing High-Tech Crime), Belgrade, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.

[5] Republic of Serbia, *Zakon o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala* (Law on Organisation and Competences of Government Authorities Responsible for Combating High Technology Crime), "Official Gazette of RS", no. 61/05 and 104/09, Government of Serbia.

[6] Republic of Serbia, *Krivični zakonik Republike Srbije* (Criminal Code of the Republic of Serbia), "Official Gazette of RS", no. 85/05, 88/05 – correction, 107/05 – correction, 72/09, 111/09, 121/12, 104/13, 108/14, and 94/16, Government of Serbia.

[7] Republic of Serbia, *Zakonik o krivičnom postupku* (Criminal Procedure Code), "Official Gazette of RS", no. 72/11, 101/11, 121/12, 32/13, 45/13 and 55/14, Government of Serbia.

[8] Ministry of Interior, *Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine i Akcioni plan 2019–2020. za sprovođenje strategije za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine* (Strategy for Combating High-Technology Crime for 2019-2023 and Action Plan 2019-2020 for Implementing the Strategy for Combating High-Technology Crime for 2019-2023), Government of Serbia, available at: http://www.mup.gov.rs/wps/portal/sr/dokumenti/Strategije, accessed: 17/03/2021.

[9] Ibid., p. 47.

[10] Ministry of Interior, *Akcioni plan za Poglavlje 24 – Pravda, Sloboda i bezbednost* (Action Plan for Chapter 24 – Justice, Freedom and Security), 2020, p. 186, Government of Serbia, available at: http://www.mup.gov.rs/wps/wcm/connect/534c031c-49b6-4e09-bd14-20a80e72778e/Akcioni+plan+za+P24+-+revidirana+verzija+23+07+2020.pdf?MOD=AJPERES&CVID=ng1hMov, accessed: 17/03/2021.

[11] Interview with Lidija Komlen Nikolić, President of the Presidency of the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, conducted online via Zoom on 05/03/2021.

[12] Ministry of Interior, *Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine* (Strategy for Combating High-Technology Crime for 2019-2023), Government of Serbia, p. 25.

[13] Ibid., p. 25.

[14] The 2020 reorganisation of the Department for High-Tech Crime increased the number of personnel at the Department from 16 to 22, while the Special Prosecution for High-Tech Crime increased its personnel from 11 to 13. These data can be found in the Strategy for Combating High-Technology Crime for 2019-2023, p. 24-25.

[15] Statistical data from the Statistical Office of the Republic of Serbia show that criminal acts pertaining to the offence of endangerment of safety have been on the increase for three years (2017, 2018 and 2019). On average it's about 3300 cases per year. On the other hand, offences pertaining to data security were as follows: 7 offences in 2019, 11 in 2018 and 22 in 2017. These data are available at: https://www.stat.gov.rs/oblasti/pravosudje/, accessed: 17/03/2021.

[16] Interview with Lidija Komlen Nikolić, President of the Presidency of the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, conducted online via Zoom on 05/03/2021.

[17] EUROPOL, *Internet Organised Crime Threat Assessment,* 2020, p. 8, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, accessed: 17/03/2021.

[18] Ministry of Interior, *Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. Godine* (Strategy for Combating High-Technology Crime for 2019-2023), Government of Serbia, p. 27.

[19] Republic of Serbia, *Zakon o bezbednosnu-informativnoj agenciji* (Law on the BIA), "Official Gazette of RS", no. 42/02, 111/09, 65/14 – US, 66/14 and 36/18, Government of Serbia.

[20] Republic of Serbia, *Zakon o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji* (Law on the VBA and VOA), "Official Gazette of RS", no. 88/09, 55/12 – US and 17/13, Government of Serbia.

[21] Ministry of Interior, *Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. Godine* (Strategy for Combating High-Technology Crime for 2019-2023), Government of Serbia, p. 26.

[22] Williams, P. 2001, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*,Available at: https://www.crime-research.org/library/Cybercrime.htm, accessed: 17/03/2021.

[23] Viano, C. E. et. al. 2017, Washington DC, *Cybercrime, Organized Crime, and Societal Responses,* Springer.

[24] RTS, *Specijalna emisija* (Special Programme), https://www.rts.rs/page/stories/ci/story/124/drustvo/4284838/belivuk-istraga-prisluskivanje-organizovani-kriimnal.html, accessed: 17/03/2021.

[25] The term avatar indicates a virtual identity used by individuals in online spaces, usually expressed as a nickname used by the individual and behaviour exhibited by the individual online. Avatars are used to maintain privacy online but also to establish a reputation. In the hacker community, avatars are literally the identities of hackers and are linked to their reputation.

[26] Ministry of Interior, *Procena pretnje od teškog i organizovanog kriminala – SOCTA* (Serious and Organised Crime Threat Assessment – SOCTA), 2019, p. 113, available at: http://www.mup.gov.rs/wps/wcm/connect/fb61b551-a863-42b3-a208-53892082f851/SOCTA+2019+-+Procena+pretnje+od+teskog+i+organizovanog+kriminala.pdf?MOD=AJPERES&CVID=nl6aHQ2, accessed: 17/03/2021

[27] Williams, P. 2001, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Available at: https://www.crime-research.org/library/Cybercrime.htm, accessed: 17/03/2021.

BCSP

bezbednost.org

WESTERN BALKANS
ORGANIZED CRIME
RADAR

radar.bezbednost.org